AMENDMENTS TO THE CLAIMS

Claims 1-7 (canceled).

8. (New) A quantum key distributing method of correcting an error of reception data with probability information obtained as a result of measurement of a photon on a quantum communication path to estimate original transmission data and using a result of the estimation as shared information, the quantum key distributing method comprising:

first error-correction-information notifying including

a transmission-side communication apparatus notifying a reception-side communication apparatus of first error correction information generated based on a second parity check matrix and the transmission data, via a public communication path, the second parity check matrix, which is identical in both of the communication apparatuses, corresponding to a specific coding rate within a desired range, and being extracted from a first parity check matrix that is identical in both of the communication apparatuses, and is optimized at a coding rate in the desired range;

first error correcting including

the reception-side communication apparatus correcting an error of the reception data based on the first error correction information;

second error-correction-information notifying including

the transmission-side communication apparatus notifying the reception-side communication apparatus of additional second error correction information generated based on a third parity check matrix and the transmission data, via the public communication path, the third parity check matrix, which is identical in both of the communication apparatuses, corresponding to a coding rate lower than a last coding rate, and being extracted, when the error of the reception data is

not completely corrected, from the first parity check matrix such that last error correction information becomes a part of information at a time of next error correction;

second error correcting including

the reception-side communication apparatus correcting the error of the reception data based on the first error correction information and the second error correction information; and

encryption-key generating including, when the error of the reception data is completely corrected at the first error correcting or when the error is completely corrected by repeatedly executing the second check-matrix generating, the second error-correction-information notifying, and the second error correcting,

discarding a part of shared information according to an amount of opened error correction information; and

setting a result of the discarding as an encryption key.

9. (New) The quantum key distributing method according to claim 8, wherein

the first parity-check-matrix generating includes

determining a code length and a coding rate in the desired range;

fundamental-matrix generating including

selecting a matrix forming a basis of the first parity check matrix satisfying conditions that weights of rows and columns are fixed and number of cycles on a bipartite graph is equal to or larger than six; and

generating a first fundamental-matrix corresponding to an upper limit value in the desired range and a second fundamental-matrix corresponding to a lower limit value in the desired range, based on the selected matrix;

check-matrix generating including

optimizing an order allocation of a weight of a row and a weight of a column of a parity check matrix corresponding to the upper limit value by executing Gaussian approximation based on upper limit values of the code length and the coding rate; and

generating a parity check matrix corresponding to the upper limit value of the coding rate by dividing at least one of a row weight and a column weight of the first fundamental-matrix based on the optimized order allocation, and

additional-matrix generating including

optimizing an order allocation of a weight of a row and a weight of a column of a parity check matrix corresponding to the lower limit value under a constraint that a parity check matrix corresponding to the upper limit value is included, by executing the Gaussian approximation based on the lower limit value of the coding rate; and

generating an additional matrix with respect to the parity check matrix corresponding to the upper limit value by dividing at least one of a row weight and a column weight of the second fundamental-matrix based on the optimized order allocation, and

a parity check matrix corresponding to the lower limit value in which the parity check matrix corresponding to the upper limit value and the additional matrix are connected is set as the first parity check matrix.

10. (New) The quantum key distributing method according to claim 8, wherein

the first check-matrix generating includes

determining a code length and a coding rate in the desired range;

fundamental-matrix generating including

selecting a matrix forming a basis of the first parity check matrix satisfying conditions that weights of rows and columns are fixed and number of cycles on a bipartite graph is equal to or larger than six; and

generating a fundamental-matrix corresponding to an upper limit value in the desired range and fundamental-matrixes, which includes a fundamental-matrix corresponding to a lower limit value in the desired range, corresponding to a plurality of coding rates set stepwise in the range, based on the selected matrix;

check-matrix generating including

optimizing an order allocation of a weight of a row and a weight of a column of a parity check matrix corresponding to the upper limit value by executing Gaussian approximation based on upper limit values of the code length and the coding rate; and

generating a parity check matrix corresponding to the upper limit value of the coding rate by dividing at least one of a row weight and a column weight of the first fundamental-matrix based on the optimized order allocation; and

additional-matrix generating including

optimizing an order allocation of a weight of a row and a weight of a column of a parity check matrix corresponding to the coding rate under a constraint that a parity check matrix corresponding to the coding rate at one stage higher is included, by executing the Gaussian approximation based on a coding rate at one stage lower than a last coding rate; and

generating an additional matrix with respect to a parity check matrix corresponding to a coding rate at one stage higher by dividing at least one of a row weight and a column weight of a fundamental-matrix corresponding to a coding rate at one stage lower based on the optimized order allocation,

the additional-matrix generating is repeatedly executed until the coding rate reaches a coding rate corresponding to the lower limit value while decreasing the coding rate, and

a parity check matrix corresponding to the lower limit value in which the parity check matrix corresponding to the upper limit value and all additional matrixes are connected is set as the first parity check matrix.

11. (New) The quantum key distributing method according to claim 9, wherein

a Euclidian geometric code is used as a matrix satisfying the conditions that the weights of rows and columns are fixed and the number of cycles on the bipartite graph is equal to or larger than six.

12. (New) The quantum key distributing method according to claim 10, wherein

a Euclidian geometric code is used as a matrix satisfying the conditions that the weights of rows and columns are fixed and the number of cycles on the bipartite graph is equal to or larger than six.

13. (New) A reception-side communication apparatus that corrects an error of reception data with probability information obtained as a result of measurement of a photon on a quantum communication path to estimate original transmission data and using a result of the estimation as shared information to be shared with a transmission-side communication apparatus, the reception-side communication apparatus comprising:

a decoding unit that corrects the error of the reception data based on a second parity check matrix and error correction information received from the transmission-side communication

apparatus via a public communication path, the second parity check matrix, which is identical in both of the communication apparatuses, corresponding to a specific coding rate within a desired range, and being extracted from a first parity check matrix that is optimized at a coding rate in the desired range; and

an encryption-key generating unit that discards a part of the shared information according to an amount of opened error correction information and sets a result of discarding as an encryption key, when the error of the reception data is completely corrected, wherein

the decoding unit corrects the error of the reception data based on a third parity check matrix and error correction information added from the transmission-side communication apparatus via the public communication path, the third parity check matrix, which is identical in both of the communication apparatuses, corresponding to each coding rate, and being extracted, when the error of the reception data is not completely corrected, from the first parity check matrix such that last error correction information becomes a part of information at a time of next error correction while decreasing the coding rate.

14. (New) The reception-side communication apparatus according to claim 13, further comprising:

a check-matrix generating unit that extracts the second parity check matrix from the first parity check matrix, and extracts the third parity check matrix, when the error of the reception data is not completely corrected, from the first parity check matrix such that the last error correction information becomes the part of information at the time of next error correction while decreasing the coding rate.

15. (New) A transmission-side communication apparatus that uses, when a reception-side communication apparatus estimates original transmission data from reception data with probability information obtained as a result of measurement of a photon on a quantum communication path, a result of the estimation as shared information to be shared with the reception-side communication apparatus, the transmission-side communication apparatus comprising:

an error-correction-information generating unit that generates error correction information based on a second parity check matrix and the transmission data and notifies the reception-side communication apparatus of a result of generating the error correction information via a public communication path, the second parity check matrix corresponding to a specific coding rate within a desired range, and being extracted from a first parity check matrix that is optimized at a coding rate in the desired range; and

an encryption-key generating unit that discards a part of the shared information according to an amount of opened error correction information and sets a result of discarding as an encryption key, when the error of the reception data is completely corrected, wherein

the error-correction-information generating unit notifies the reception-side communication apparatus of additional error correction information via the public communication path until the error of the reception data is completely corrected, based on a third parity check matrix, which is identical in both of the communication apparatuses, corresponding to each coding rate, the third parity check matrix being extracted, when the error of the reception data is not completely corrected, from the first parity check matrix such that last error correction information becomes a part of information at a time of next error correction while decreasing the coding rate.

16. (New) The transmission-side communication apparatus according to claim 15, further

comprising:

a check-matrix generating unit that extracts the second parity check matrix from the first parity check matrix, and extracts the third parity check matrix, when the error of the reception data is not completely corrected, from the first parity check matrix such that the last error correction information becomes the part of information at the time of next error correction while decreasing the coding rate.